DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Name of MACOM/DA Staff Proponent (APMS Sub Organization Name)

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (FMWRC)

2. Name of Information Technology (IT) System (APMS System Name)

Time Labor Management System (TLMS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR).

4016

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0215-1a SAFM Nonappropriated Funds Central Payroll System (NAFCPS) (February 22, 1993, 58 FR 10002).

7. OMB Information Collection Requirement Number (if applicable) and expiration date.

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 2105, 5531, 5533;
10 U.S.C. 3013, Secretary of the Army;
Public Law 92-203;
Fair Labor Standards Act; and
E.O. 9397 (SSN).

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

TLMS is the time and attendance software that Army Non-Appropriated Fund has used worldwide since 1985. It is a commercial-off-the -shelf (COTS) application. TLMS is the Army term for the software. Source Time is the commercial name. Source Time version 520 is the standalone version. Source Time version 550 is the SQL network version. The software is used to collect time and attendance data either from a data collection terminal or based on employee work schedules stored in the system. It is a Windows(r)-based software system. It calculates employee work hours for payroll and labor management purposes. It enables managers, supervisors and other pay/time personnel to manage employees more efficiently by providing a cost-effective method of gathering, analyzing, and reporting labor data. Source Time incorporates a database and pay rule architecture to optimize all functions related to time and attendance accounting. Source Time contains integrated review and approval capabilities designed specifically for supervisors, managers and pay/time personnel. It provides a robust reporting capability. Business rule definition capabilities eliminate rule misinterpretation and provide consistency in pay/time allocation. Source Time can run on stand-alone PCs, multi-user workstations/servers in LAN environments, or SQL Server version 7 client/server environments. It is a Windows based application that requires password authentication. The Security Groups feature controls employee access rights to the Employee module. Employees can access the employee module on one of two levels – full rights, or view only. With full rights access, employees may add and edit information that appears on their timecards, but in view only mode, they use the Employee module only to view timecard data to verify that it is correct. The employees' supervisors, payroll clerk, or system administrator must perform editing. A personal computer, Source Time software and a printer are the minimum hardware and software components required to use and maintain the Source Time system. The MWR MIS AIS forms a central point of ingress to the base network for MWR activities on that installation. The MIS is a current software system in the operational phase of its system life cycle and is upgraded as required by engineering change proposals (ECP). The system owner is US Army FMWRC. The MWR MIS Automated Information Systems forms the central point for network services and database control for the MWR MIS network. This "sub" network connects to the base network over a connection provided by, and the responsibility of, the installation DOIM. Connections between remote terminals and the MWR MIS AIS can made directly over links provided by the installation Director of Information Management (DOIM), or entire facilities can be linked to the base network and routed back to the MWR MIS AIS.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Name, Social Security, grade/rank, work center, work schedule, leave earned and taken, leave balances, address, deductions, rates of pay, bank account numbers, bank routing numbers, date of birth, user id and password. The original data is entered by the servicing Civilian Personnel Office during in-processing of the employee. Thereafter, the data is updated biweekly by a download of the Master Employee Record from the Defense Finance and Accounting Service, Non-Appropriated Fund Civilian

Payroll office, Texarkana, Texas. The employee's supervisor or timekeeper is responsible for entering the actual time worked and leave information via keyboard entry directly into the system or downloaded from a time clock.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Information is collected from the employee during in-processing and entered by the Human Resources Personnel Clerk into the appropriate forms and DCPDS and thereafter from the Master Employee Record download from DFAS NAF Civilian Payroll office. The timekeeper and supervisor input the actual time worked, leave status, or overtime via keyboard entry directly into the system or as provided by a timeclock.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

This information is needed in order to account for time and attendance and to determine proper compensation for individuals.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

The information is used to determine proper compensation for individuals based on time worked. This system also accounts for leave taken and determines employee work schedules.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Internal agency employees, authorized by role based access, such as Civilian Personnel clerks, Timekeepers and supervisors, IT system administrator. The time and attendance file from TLMS is exported to DFAS for the payment of NAF payroll. Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

The employee is given the Privacy Act Statement during in-processing and when providing updated information to the system. Providing information is voluntary, however, if the individual does not provide information they cannot be compensated.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

The Privacy Act Statement is provided by the personnel clerk during in-processing and when updating information. The statement is contained on the forms.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

User access to the data is role based. Only those users with a need-to-know will have access. Data access is controlled by rights granted and restricted according to user type; Novell security system; user ID and password and by using technologies such as data encryption and Novell Network Operating System security. The data is encrypted, access to information is controlled by user id and password, user transaction logs maintained and Novell security system is in place. Data is not released to any parties other than those with a business need to know, based on their respective rights within the application. Additionally, the security measures in place within the security configuration of the system and on the NIPRNET are in accordance with best practices and due diligence.

This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

Security activities regularly performed during the operational phase of the system life cycle focus on maintaining system security to ensure that accredited safeguards and security control system enhancements are functioning properly. Since the MIS is composed of Commercial Off The Shelf (COTS) products, the security activities of preceding phases (i.e., design and development) are incorporated into the certification and accreditation (C&A) process as required.

All systems that connect to the MWR MIS AIS must use a Novell authentication. Backup of system and data files is accomplished weekly, and incremental backups of data files are done daily. These backups are conducted according to instructions provided in the NetWare product documentation. Both full and incremental backup media are stored securely off-site and in fireproof containers. Local copies of backup data may be held provided they are similarly secured and protected. Copies of all applications and current patches are kept updated and stored offsite in fireproof containers.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A published SORN currently exists.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing individual the opportunity to object or consent,

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only; the PIA may be published in full.